SECRET
NOFORN

4 FEB 1986

The Director of Central Intelligence

Washington, D.C. 20505

LOGGED Prod 12-2C

Intelligence Community Staff

DCI/ICS 86-4010
17 JAN 1986

MEMORANDUM FOR: See Distribution

FROM: [redacted] 25X1
Chairman, DCI Intelligence Information Handling Committee

SUBJECT: Guidance on Format for Response to a HAC-Requested Report on Security Implications of Expanded Use of Computers and Office Automation Equipment

REFERENCE: Classified Annex to House Appropriation Committee Report on the FY86 DoD Appropriation Bill, dtd 28 Oct 1985, BYE-2012/85, pp. 17 and 18

1. Per reference, the HAC directed that a report be submitted by 1 March 1986 outlining the actions being taken by each Intelligence Community (IC) and Department of Defense (DoD) component to strengthen physical and electronic computer and automated office equipment security. A sanitized copy of the HAC request is at Attachment 1. (S/NF)

2. The IC Staff will consolidate responses and submit the requested report to the HAC. The HPSCI and SAC have requested copies of the responses to this HAC tasking in lieu of establishing separate reporting requirements on this subject. (S/NF)

3. The focus of the HAC request is on security procedures that IC and DoD components have instituted to protect against the opportunities for disloyal employees to compromise or steal a tremendous amount of sensitive intelligence data which is available in concise form on word processors and small computers. The HAC cites the Walker and other recent espionage cases as prompting its concern and requests that the report specifically address changes which may be needed in intra-office procedures to minimize security risks associated with increasingly transportable disks, tapes, etc. containing substantial amounts of sensitive information. (S/NF)

4. In order to respond to the Congressional Committees, it is requested that input be provided to the IC Staff NLT 10 February 1986 in the format at Attachment 2. This request for input is not intended to create the need to develop a detailed data call to working level components. Much of the requested information may be available from component responses to recent SECDEF and OMB/NSDD-145 data calls that were conducted during the past 18 months. (C)

[redacted] 25X1

SECRET

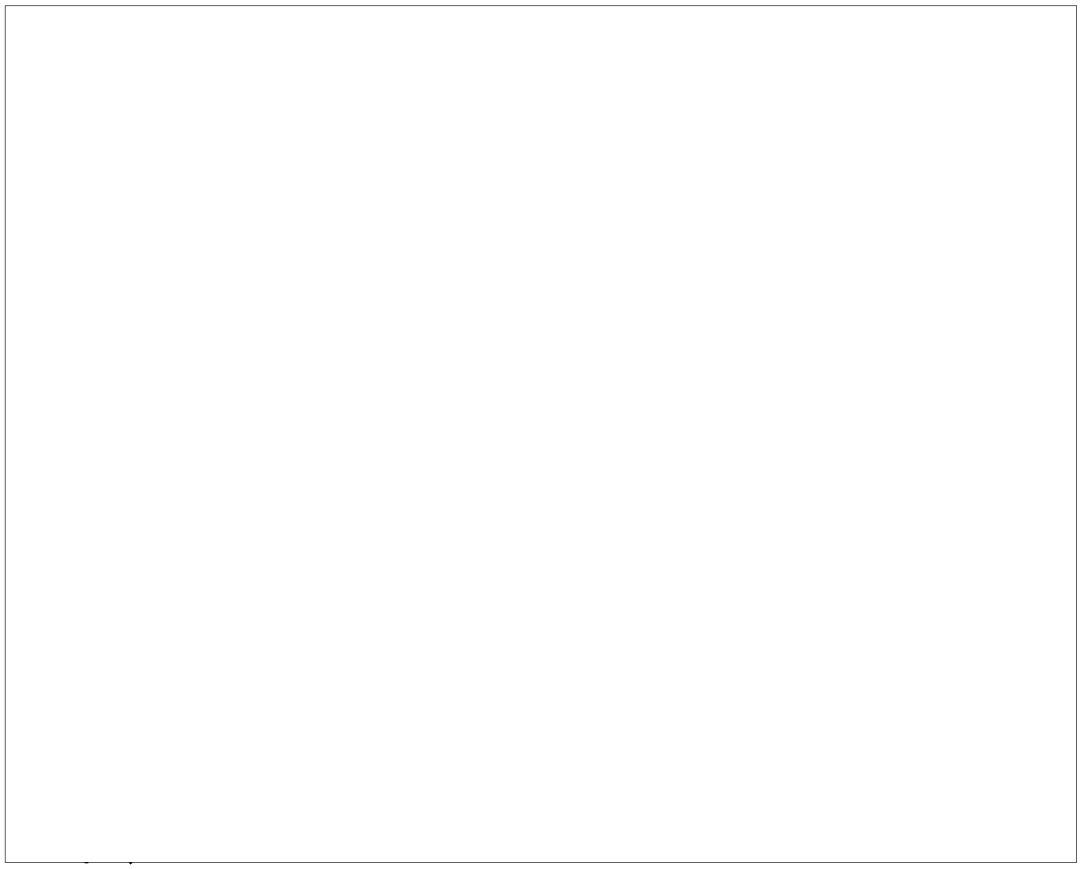
SUBJECT: Guidance on Format for Response to a HAC-Requested Report on Security Implications of Expanded Use of Computers and Office Automation Equipment

5. Input provided to the IC Staff should be in summary form and limited to two pages. Questions regarding this action should be addressed to [redacted] 25X1
[redacted] 25X1

Attachments:
As stated

NOFORN

SUBJECT: Guidance on Format for Response to a HAC-Requested Report on Security Implications of Expanded Use of Computers and Office Automation Equipment



25X1

Attachment 1

Security Implications of Expanded Use of Computers and Automated Office Equipment

The Committee notes that extensive use is made of automated data processing equipment and other equipment, such as word processors, within the Intelligence Community. The Committee is basically supportive of these efforts to procure this equipment which is beneficial to the productivity of the many offices where it is now operational.

However, the Committee is concerned about the security implications of the widespread use of the equipment. A major effort has been and is being accomplished to have much of this equipment "TEMPEST" proof--i.e. [redacted] 25X1 25X1 However, as the Walker case, and other recent espionage cases 25X1 have shown, there is a very great danger of sensitive data being provided to hostile powers by American civilians or military personnel. Thus, while technological improvements have enhanced the capability of equipment to resist the attempted electronic exploitation of that equipment by hostile powers, the improvements in performance and capability of much of the new equipment has brought forth a situation where large amounts of sensitive data could be easily exploited by disloyal Americans.

A recent Air Force audit on small computers (Project 3120115, June 11, 1984) stated the following regarding computer systems: "While offering a powerful new tool, these small computers bring with them varied concerns about implementing control techniques to protect equipment and files; prevent unauthorized processing; and ensure continued accurate, timely, secure, and complete processing of data." The report states that the Air Force alone will soon have as many as 6,000 small computers in its inventory.

The use of word processors has been very beneficial to the productivity of numerous offices. However, the Committee notes that the use of this equipment in the Intelligence Community has brought forth a situation where enormous amounts of very sensitive data are contained on one small disk. For example, one of the recent generations of word processors has up to 128 pages of data on one paper thin disk. Thus, the opportunity for a disloyal employee to compromise or steal sensitive data is greatly simplified unless the proper intra-office security measures are maintained.

The Committee fully recognizes the vital contribution the new generation of equipment is making to the intelligence effort. Indeed, many of the vital systems of the Intelligence Community could not operate without this equipment. The Committee has no intention of turning the clock back on the continued progress being made by the expanded use of this equipment. However, the combination of tremendous amounts of sensitive data being available in very concise forms, along with the dismaying fact that a few disloyal Americans may be willing to sell information to hostile foreign powers, must be taken into full consideration in the development and implementation of security procedures for individual offices.

In light of the enormous resources invested in computers and automated office equipment, and the vast potential for security compromise, the Committee directs that a report be submitted by March 1, 1986, outlining the actions being taken by each Intelligence Community and Defense Department component to strengthen physical and electronic computer and automated office equipment security. In addition, the report should also specifically address changes needed in intra-office procedures to minimize security risks associated with increasingly transportable disks, tapes, etc., which may contain substantial amounts of sensitive information.

Attachment 2

Implications of Expanded Use of
Computers and Automated Office Equipment
Processing Intelligence Information

COMPONENT: _____ DATE: _____

I. BACKGROUND INFORMATION AND SCOPE OF THE AREA OF CONCERN IDENTIFIED BY HAC

- Provide background information on the general organizational components that are included in the responses (e.g., GDIPs consolidated response may include DIA, the U&S Commands, and the non-cryptologic components of the services).

- Provide trend information (i.e., past three years and next three years, with 1985 considered the current year) as part of a general estimate of the number of word processors and small computers used by each IC and DoD component to process intelligence information. The HAC request includes a general estimate of the number of small computers in the Air Force inventory (i.e., 6,000). Responses should include round estimates of the number of such systems processing intelligence information.

- Provide trend information (i.e., past three years and next three years, with 1985 considered the current year) on the estimated increase in the storage capabilities provided by these word processors and small computers. The HAC request cited as an example of its concern that "one of the recent generations of word processors has up to 128 pages of data on one paper thin disk. Thus the opportunity for a disloyal employee to compromise or steal sensitive data is greatly simplified unless the proper intra-office security measures are maintained."

- Responses should include a general assessment of the range of storage capabilities provided by the word processors and small computers used by intelligence components (e.g., three years ago the majority of our systems used floppy disks, each capable of storing 75 pages of information per work station. Procurements over the next three years include replacing these systems with floppy disks and hard disks that can store up to 1,500 pages of information per work station). Since the HAC used number of pages of storage as an example of its concern, please use this metric whenever possible. Other examples of metrics could be: the number of documents, the number of messages, or the total number of characters stored on these systems.

II. ASSESSMENT OF THE CURRENT RISKS ASSOCIATED WITH USING THESE SYSTEMS AND A GENERAL DESCRIPTION OF SECURITY MEASURES EMPLOYED TO LIMIT THE RISKS

- Provide a summary of the assessment of risks associated with using this equipment. Risk statements in this area may include considerations of personnel, physical, administrative and procedural, and technical security measures. The following is provided as a general guideline for information to be included in the response:

  Word processors and small computers have little or no technical security features as part of their basic design. The risks associated with this has been balanced with the operational need to store the indicated amount of information on these systems. As part of this risk assessment, the technical security limitations of these systems have been addressed by improving administrative and procedural security measures including the labelling of all storage devices and by the development of security features on the mainframe computer equipment to which many of these devices are attached. In addition, these devices are used in "closed environments" protected by those physical and personnel security techniques that traditionally have been used to protect the information processed in hardcopy form. The volume and sensitivity of information available on these devices dictates that all forms of security be employed to limit the risk while providing the processing capabilities required to satisfy operational needs.

- The responses should address both the technical and non-technical security measures employed to protect intelligence information processed by these systems. If protection of the information is more dependent on one area of security than others, this should be highlighted in the response (e.g., physical and personnel security are the basis of the security measures employed to protect the information. Technical measures and administrative and procedural controls supplement the physical and personnel security measures).

- Highlight current procedures to minimize perceived security risks associated with increasingly transportable disks, tapes, etc., which may contain substantial amounts of sensitive information. Include general descriptions of procedures for labelling, controlling, and accounting for such information.

- Summarize current efforts to provide for maintenance of the current number of such systems and any problems that may be caused by the number of future systems.

III. SUMMARY OF ON-GOING EFFORTS TO REDUCE THESE RISKS HIGHLIGHTING ANY SHORTFALLS THAT NEED TO BE ADDRESSED

- Include a description of ongoing and proposed efforts to reduce these risks and indicate whether there are resource shortfalls (including personnel) that may prevent implementation of appropriate security measures. The response should include a statement of the adequacy of the resources in the program and budgets of the components (i.e., are there sufficient resources in the program and budget of the NFIP to operate these systems at the level of risk described above).